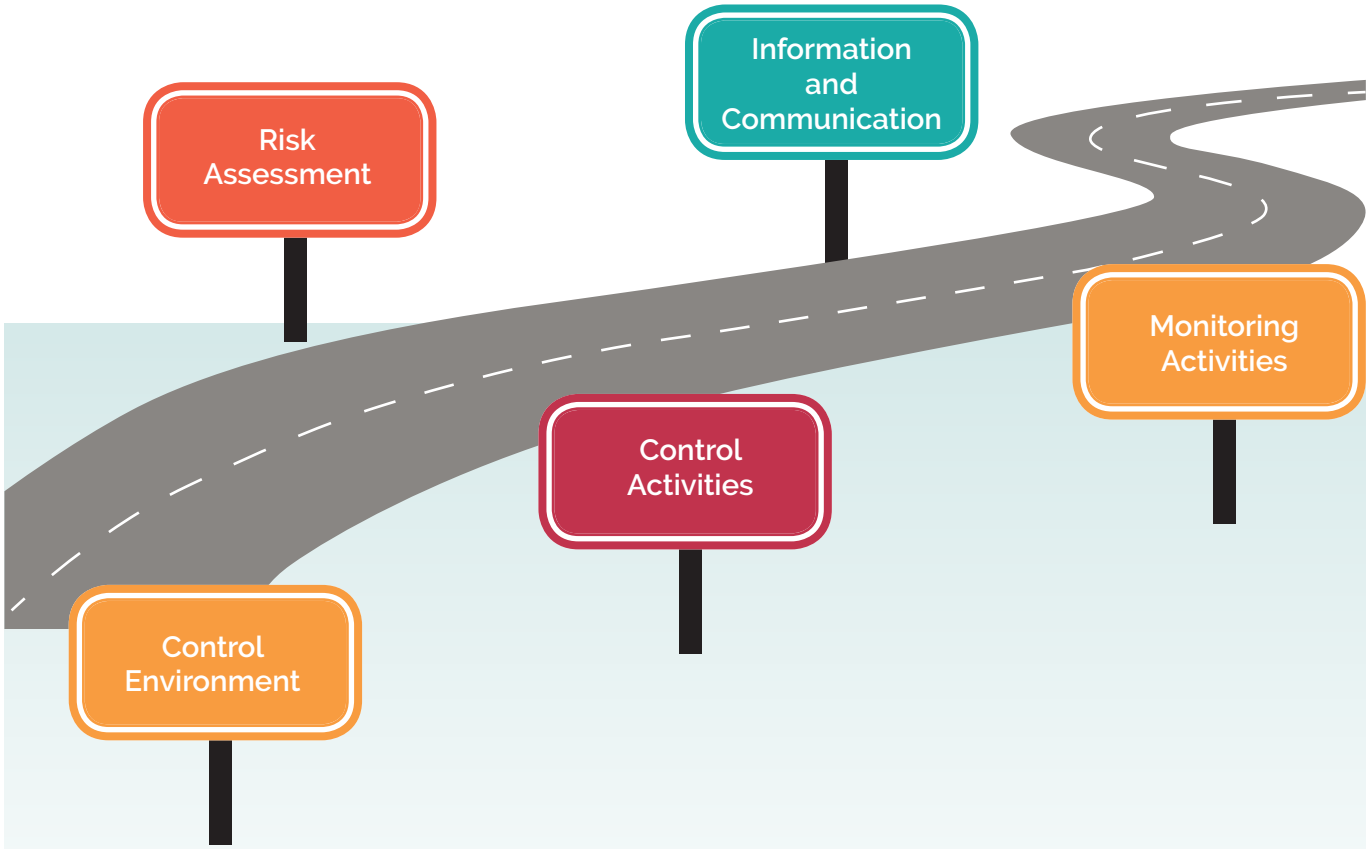
ICE
Integrated Control Environment



CONTROL ENVIRONMENT SELF-ASSESSMENT QUESTIONNAIRE

The starting point to a comprehensive review and analysis of your company's risk and control environment

www.ice-control.co.uk

CONTROL ENVIRONMENT SELF-ASSESSMENT

Introduction 3

How to Use this Questionnaire 4

Control Environment 5
- Integrity and Ethics
- Independence and Oversight
- Organisational Structure
- Recruitment and Staffing
- Individual Responsibilities

Risk Assessment 10
- Organisation Objectives
- Identification and Management
- Fraud
- Assessing Changes

Control Activities 14
- Developing Controls
- Technology Controls
- Policies and Procedures

Information and Communication 18
- Provision of Information
- Internal Communication
- External Communication

Monitoring Activities 21
- Ongoing Evaluation
- Deficiency Management

About ICE Integrated Control Environment 23

How This Questionnaire Can Help You

Control Environment Self-Assessment

This questionnaire is the starting point to help you undertake a comprehensive review and analysis of your company's risk and control environment. It is based on the model devised by the *Committee of Sponsoring Organizations of the Treadway Commission* (COSO), the globally recognised body that is dedicated to risk management and internal control.

It contains over 200 questions to help you critically appraise your company's current control environment, reflect on what is operating well, and devise a plan of action for improvements going forward.

If you would like a professional review, or would like to discuss your findings of this self-assessment, contact:

Ross Baptie, Design & Delivery Director, ICE Integrated Control Environment
Ross.Baptie@ice-control.co.uk

ICE
Integrated Control Environment

How To Use This Questionnaire

The questionnaire is split into five key components or 'pillars', each containing individual principles. Questions are then asked for each principle, scoring each from 0 to 10. For each principle, calculate an overall percentage to assess your company's performance.

These questions are a first step – the key is to then analyse the results and determine where your company has specific areas of weakness and what actions need to be taken to improve your control environment.

Since some of the questions may have greater significance to your organisation, you may wish to weight the questions when determining an overall assessment for a specific principle or category.

OVERVIEW OF QUESTIONNAIRE STRUCTURE AND PRINCIPLES

Control Environment	Risk Assessment	Control Activities	Information & Communication	Monitoring Activities
• Integrity and Ethics • Independence and Oversight • Organisational Structure • Recruitment and Staffing • Individual Responsibilities	• Organisation Objectives • Identification & Management • Fraud • Assessing Changes	• Developing Controls • Technology Controls • Policies and Procedures	• Provision of Information • Internal Communication • External Communication	• Ongoing Evaluation • Deficiency Management

CONTROL ENVIRONMENT: Integrity and Ethics

The organisation demonstrates a commitment to integrity and ethical values.

Ref	Question	Scoring
1.1	Is the board of directors and management's commitment to integrity and ethical behaviour communicated effectively throughout the organisation, both in words and deeds? Do the board of directors and management lead by example?	
1.2	Is the tone set by the board of directors and senior management communicated through to various operating units? Do such communications consider the various factors, including potential barriers, that may be present at each unit (e.g. cultural, language)?	
1.3	Is the tone exhibited by management of operating units consistent with that set by the board of directors and senior management?	
1.4	Is there a code of conduct and/or ethics policy and has it been adequately communicated to all levels of the organisation?	
1.5	If there is a code of conduct, does it provide standards to guide the organisation's behaviours, activities and decisions by doing the following things?	
1.5.1	Establishing what is right and wrong?	
1.5.2	Reflecting local laws, rules, regulations, standards and other	
1.5.3	Expectations that the organisation's stakeholders may have	
1.5.4	Meeting the specific needs of various operating units (e.g. based on market, culture, language) so it can be consistently implemented throughout the organisation?	
1.6	Is the organisation's commitment to integrity and ethical behaviour regularly communicated to joint venture partners, suppliers, sales distributors, outsourced service providers and other business partners?	
1.7	Are those in top management hired from outside made familiar with the importance of high ethics and controls?	
1.8	Is the organisation's commitment to integrity and ethical behaviour included in training for new employees and contractors?	
1.9	Does the organisation have a process in place to communicate standards of conduct throughout the organisation, including external partners/outsourced service providers?	
1.10	Does the organisation have a process to evaluate the performance of individuals and teams against its standards of conduct? Does it consist of the following:	
1.10.1	Continual and periodic compliance procedures	
1.10.2	Consideration of integrity and ethical values in performance	
1.10.3	Reviews, compensation and promotion decisions	
1.10.4	Investigation of allegations of noncompliance of its standards of conduct by independent personnel	
1.11	Has the organisation established tolerance levels for deviations to its standards of conduct? Are such tolerance levels communicated throughout the organisation? Are deviations evaluated in a timely manner?	
1.12	Does the organisation periodically analyze issues to identify trends and root causes to evaluate whether modification of policies, communication, training or controls are necessary?	

Scoring Guidelines: 10 Strongly Agree; 7 Mostly Agree; 5 Neither Agree nor Disagree; 3 Mostly Disagree; 0 Strongly Disagree

CONTROL ENVIRONMENT: Independence and Oversight

The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.

Ref	Question	Scoring
2.1	Is the makeup of the board of directors, including the number of directors and their background and expertise, appropriate given the nature of the organisation?	
2.2	Are the makeup and skills of the board members periodically evaluated to assure that directors have the expertise to ask probing questions of management and to take appropriate actions?	
2.3	Do board members participate in training as appropriate to keep their skills and expertise current and relevant?	
2.4	Has the independence of outside board members been adequately reviewed, including affiliations and relationships and transactions with the organisation or other organisations that could result in a conflict of interest?	
2.5	Does the audit committee have a charter outlining its duties and responsibilities?	
2.6	Does the audit committee have adequate resources and authority to discharge its responsibilities	
2.7	Is the board of directors or audit committee an informed, vigilant and effective overseer of the financial reporting process and the organisation's internal control, including technology and relevant risks and controls?	
2.8	Does the board of directors or audit committee maintain a direct line of communication with the entity's external and internal auditors?	
2.9	Does the board of directors or the audit committee stay abreast with current internal control practices in the entity as well as the industry, and is it aware of recent regulations and changes that affect the overall system of internal control at the organisation?	

Scoring Guidelines: 10 Strongly Agree; 7 Mostly Agree; 5 Neither Agree nor Disagree; 3 Mostly Disagree; 0 Strongly Disagree

CONTROL ENVIRONMENT: Organisational Structure

Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.

Ref	Question	Scoring
3.1	Is the organisational structure appropriate for the size, operating activities and locations of the organisation to enable management to carry out their oversight responsibilities?	
3.2	Does management review and make modifications to the organisational structure of the organisation in light of changed conditions or revised priorities?	
3.3	Are the reporting lines clear and appropriate to enable accountability over operating units and functional areas?	
3.4	Are reporting lines evaluated periodically, and do they enable the execution of authorities and responsibilities and the flow of information to manage the entity's activities?	
3.5	Are job descriptions that outline financial reporting responsibilities maintained and updated when necessary?	
3.6	Are there adequate policies and procedures for authorisation and approval of transactions by the appropriate level?	
3.7	Is there an appropriate structure for assigning ownership of data, including who is authorised to initiate and/or change transactions? Is ownership assigned for each application and database within the IT infrastructure?	
3.8	Is there an appropriate segregation of incompatible activities (i.e., separation of accounting for, and access to, assets) both physically and through access to the IT systems?	
3.9	Are the contractual terms with outsourced service providers clear and concise with regard to the organisation's objectives and expectations of conduct and performance, competence levels and expected information and communication flow?	
3.10	Are there appropriate policies for matters such as accepting new business, conflicts of interest and security practices? Are they adequately communicated throughout the organisation?	

Scoring Guidelines: 10 Strongly Agree; 7 Mostly Agree; 5 Neither Agree nor Disagree; 3 Mostly Disagree; 0 Strongly Disagree

CONTROL ENVIRONMENT: Recruitment and Staffing

The organisation demonstrates a commitment to attract, develop and retain competent individuals in alignment with objectives.

Ref	Question	Scoring
4.1	Are there standards and procedures for hiring, training, motivating, evaluating, promoting, compensating, transferring and terminating the employment of personnel that are applicable to all functional areas?	
4.2	Are there screening procedures for job applicants?	
4.3	Does the organisation have policies and practices to articulate the skills, competencies and behaviours that should be in place at all levels of the organisation, including outsourced service providers?	
4.4	Are there written job descriptions, reference manuals or other forms of communication to inform personnel of their duties?	
4.5	Are there periodic evaluations of departmental staffing needs (particularly with regard to knowledge and experience of management and supervisory levels within the accounting, information systems and financial reporting areas)?	
4.6	Does management demonstrate a commitment to provide sufficient accounting and financial personnel to keep pace with the growth and/or complexity of the business?	
4.7	Are training needs identified and delivered to requisite personnel to address needs such as emerging standards or other areas where improvement is needed?	
4.8	Does management set expectations that personnel raise issues or questions relating to significant financial reporting or internal control issues?	
4.9	Does the organisation have a formal process to evaluate performance & competence and take remedial actions for any issues identified?	
4.10	Do the entity's policies include succession plans for senior executives and contingency plans for assignments of responsibilities important for internal control?	

Scoring Guidelines: 10 Strongly Agree; 7 Mostly Agree; 5 Neither Agree nor Disagree; 3 Mostly Disagree; 0 Strongly Disagree

CONTROL ENVIRONMENT: Individual Responsibilities

The organisation holds individuals accountable for their internal control responsibilities in the pursuit of objectives.

Ref	Question	Scoring
5.1	Does the organisation's structure and tone at the top help establish and enforce individual accountability for performance of internal control responsibilities? Does it communicate and reinforce the accountability for responsible conduct of all personnel?	
5.2	Is there a mechanism in place to regularly educate and communicate, to management and employees, the importance of internal controls, and to raise their level of understanding of internal control?	
5.3	Does management have processes and controls in place to evaluate and hold outsourced service providers (and other business partners) accountable for their internal control responsibilities?	
5.4	Does the organisation provide measures, incentives and other rewards that are aligned with ethical values and performance related to internal control, including financial and nonfinancial measures?	
5.5	Does management set realistic (i.e., not unduly aggressive) financial targets and expectations for operating personnel?	
5.6	Are performance measures reviewed periodically for relevance and adequacy in relation to their potential risks and rewards?	
5.7	Does the board of directors and management act to remove or reduce incentives or temptations that might prompt personnel to engage in dishonest, illegal or unethical acts?	
5.8	Do management and the board of directors evaluate performance of internal control responsibilities, including adherence to standards of conduct and levels of competence? Do appropriate rewards or disciplinary actions result from such evaluations?	

Scoring Guidelines: 10 Strongly Agree; 7 Mostly Agree; 5 Neither Agree nor Disagree; 3 Mostly Disagree; 0 Strongly Disagree

RISK ASSESSMENT: Organisation Objectives

The organisation specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.

Ref	Question	Scoring
6.1	Are the external financial reporting objectives consistent with the relevant financial reporting framework and appropriate in the circumstances?	
6.2	Does management establish a materiality threshold for the purpose of identifying significant accounts and disclosures? Does this consider risks at all locations/geographies where the entity conducts activities?	
6.3	Does the organisation specify objectives by identifying the following: • Significant financial statement accounts and disclosures • Relevant assertions • Underlying transactions and events • Processes supporting those accounts and disclosures	
6.4	Do the organisation's policies, procedures and processes facilitate the development of financial statements that reflect the transactions and events that underlie them? For example, do they consider: • Relevance — information that is meaningful to users of the financial statements • Faithful representation — information that is complete, neutral and free from error • Comparability — information that facilitates comparison with other entities and with similar information from the same entity • Verifiability — information that can be substantiated • Timeliness — information that can be provided in time to be useful to users of the financial statements • Understandability — information that is presented clearly and concisely	
6.5	Does the organisation consider the factors in 6.4 above when establishing accounting policies where alternative treatments under the relevant financial reporting framework may exist?	
6.6	Does the organisation periodically review and update its understanding of the requirements of the applicable financial reporting framework?	
6.7	Does the organisation have a process to evaluate the range of its activities to assess whether all material activities are appropriately reflected in the financial statements?	

Scoring Guidelines: 10 Strongly Agree; 7 Mostly Agree; 5 Neither Agree nor Disagree; 3 Mostly Disagree; 0 Strongly Disagree

RISK ASSESSMENT: Identification and Management

The organisation identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.

Ref	Question	Scoring
7.1	Does the organisation identify risks to the achievement of financial reporting objectives at all levels of the entity (e.g. subsidiary, division, operating unit and functional levels)?	
7.2	Does the organisation's process to identify risks to the achievement of financial reporting objectives include consideration of both internal and external risk factors to each significant financial statement account or disclosure, and related assertions? Consider the following: • Quantitative and qualitative factors • Nature of account, such as volume of transactions, complexity and degree of judgment required to determine amount or disclosure • Nature of the underlying class of transactions, including whether such transaction streams are centralized or decentralized, the IT applications used, whether the transactions are subject to changes during the year, and the level of involvement and/or interaction with external parties • Risks associated with the accounting and reporting for infrequent and/or unusual transactions for which controls may not have been implemented in the normal course of business • Whether fraud risks are associated with the particular account or disclosure • Whether a new financial reporting standard or law or regulation exists that requires different or additional reporting • Impact of changing user needs or expectations on the amounts reflected in the organisation's financial statements • Changes in management responsibilities that can affect the way certain controls operate • The quality of personnel hired and the methods of training and motivation • The nature of the entity's activities and employee accessibility to assets • A disruption in information processing	
7.3	Is the risk identification comprehensive and does it include all significant interactions internal to an entity and between the entity and its relevant business partners and outsourced service providers?	
7.4	Does the organisation involve the appropriate levels of management with the necessary expertise to identify risks to achieving its financial reporting objectives, and to perform the related assessment of the risks? For example: • Are there processes to ensure the accounting department is made aware of changes in the operating environment so they can review the changes and determine what, if any, effect the change may have on the entity's accounting policies? • Are there channels of communication between the accounting department and/or individuals in charge of monitoring regulatory rules so the accounting department is aware of regulatory changes that could affect the entity's accounting policies? • Are there processes to ensure that the accounting department (and/or audit committee) is aware of significant transactions with related parties so they can determine whether such transactions are appropriately approved, accounted for and disclosed? • Does the audit committee review and approve significant changes to the organisation's accounting practices?	
7.5	Does management's risk assessment process consider the likelihood and magnitude of occurrence of an identified risk?	
7.6	Is the risk assessment revisited on an appropriate interval?	

Scoring Guidelines: 10 Strongly Agree; 7 Mostly Agree; 5 Neither Agree nor Disagree; 3 Mostly Disagree; 0 Strongly Disagree

RISK ASSESSMENT: Fraud

The organisation considers the potential for fraud in assessing risks to the achievement of objectives.

Ref	Question	Scoring
8.1	Does the organisation perform a risk assessment to consider risk related to fraudulent financial reporting, management override, potential loss of assets and corruption?	
8.2	Does the organisation's risk assessment process include an evaluation of incentives and pressures, opportunities, attitudes and rationalisations to commit fraud (e.g. reviewing incentive compensation programs to evaluate how meeting, or not meeting, financial reporting targets could provide incentives and pressures for employees to commit fraud)?	
8.3	Does the assessment of fraud risk consider opportunities for unauthorised acquisition, use, or disposal of assets, altering the organisation's reporting records or committing other inappropriate acts?	
8.4	Does the assessment of fraud risk consider the opportunities for willful violations of laws or governmental regulations that could have a material direct or indirect impact on external financial reporting?	
8.5	Does the assessment of fraud risk consider the various ways that fraudulent financial reporting could occur? For example: • Management bias • The degree of estimates and judgments in external reporting • Fraud schemes and scenarios common to the industry sectors and markets in which the organisation operates • Geographic regions where the entity does business • Incentives that may motivate fraudulent behaviour • Nature of technology and management's ability to manipulate information • Unusual or complex transactions subject to significant management influence • Vulnerability to management override and potential schemes to circumvent existing control activities	
8.6	Does the assessment of fraud risk consider how management and other personnel might engage in or justify inappropriate actions?	
8.7	Does the organisation have established procedures to periodically reconcile physical assets (e.g., cash, accounts receivable, inventories, fixed assets) with the related accounting records?	

Scoring Guidelines: 10 Strongly Agree; 7 Mostly Agree; 5 Neither Agree nor Disagree; 3 Mostly Disagree; 0 Strongly Disagree

RISK ASSESSMENT: Assessing Changes

The organisation identifies and assesses changes that could significantly impact the system of internal control.

Ref	Question	Scoring
9.1	Are there groups or individuals who are responsible for anticipating or identifying external changes with possible significant effects on the entity (e.g., regulatory or economic changes)?	
9.2	Are there processes in place to inform appropriate levels of management about changes with possible significant effects on the entity?	
9.3	Does the organisation consider the potential impact of new business lines, dramatically altered compositions of existing business lines, acquired or divested business operations, rapid growth, changing reliance on foreign geographies and new technologies on its system of internal control?	
9.4	Does the organisation have a process to consider changes in management and their respective attitudes and philosophies on the system of internal control?	

Scoring Guidelines: 10 Strongly Agree; 7 Mostly Agree; 5 Neither Agree nor Disagree; 3 Mostly Disagree; 0 Strongly Disagree

CONTROL ACTIVITIES: Developing Controls

The organisation selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.

Ref	Question	Scoring
10.1	Has the organisation undertaken a process to: • Address the identified financial reporting risks via specific responses? • Consider all the relevant business processes, information technology and locations where control activities are needed (including outsourced service providers and other business partners)? • Consider control activities to address the integrity of information sent to and received from outsourced service providers? • Consider adequacy of controls performed by outsourced service providers and other business partners? For example, has management mapped controls to address each risk related to the relevant financial statement assertions?	
10.2	Are the appropriate personnel involved in the process of designing and implementing controls to respond to the identified risks (e.g., financial personnel, internal auditors, business process owners)?	
10.3	Do the controls employed by the organisation include an appropriate mix of authorisations, approvals, comparisons, exception reporting, physical counts, reconciliations, reviews and supervisory controls?	
10.4	Are the controls employed by the organisation appropriate based on the organisation's environment, complexity, nature, scope and characteristics, as well as those of the particular business process?	
10.5	Do the controls include a range and variety of controls, including manual and automated, preventive and detective?	
10.6	Do the controls identified address the completeness, accuracy and validity of transactions processed?	
10.7	Do the controls identified include controls over the completeness, accuracy and validity of reference data used in transaction processing (e.g. a pricing master file) and the operation of other controls (e.g. reconciliation controls)?	
10.8	Has the organisation considered the precision (i.e., the degree to which controls, if operating effectively, would prevent or detect misstatements in the financial statements that could be material) of the controls when evaluating the extent to which they address the identified risks? For example, have they considered the following: • Whether the level of precision is objective (system-based) or subjective (performance of a review) • The nature of errors identified by the control • Whether there is adequate follow-up in response to discrepancies or errors identified • What evidence exists to confirm the control operated as intended	
10.9	Do controls exist at various levels within the organisation from transaction level controls to entity-level management review controls?	
10.10	Is there appropriate segregation of duties (e.g., separation of accounting for and access to assets, IT operations function separate from systems and programming, database administration function separate from application programming and systems programming)? Are organisational charts, automated tools, process flow diagrams or other tools used to ensure proper segregation of duties exist?	
10.11	Are appropriate approvals from management required prior to allowing an individual access to specific applications and databases?	
10.12	Are IT personnel prohibited from having incompatible responsibilities or duties in user departments?	
10.13	Are there processes to periodically (e.g., quarterly, semiannually) review system privileges and access controls to the different applications and databases within the IT infrastructure to determine whether system privileges and access controls are appropriate?	

Scoring Guidelines: 10 Strongly Agree; 7 Mostly Agree; 5 Neither Agree nor Disagree; 3 Mostly Disagree; 0 Strongly Disagree

CONTROL ACTIVITIES: Technology Controls (1 of 2)

The organisation selects and develops general control activities over technology to support the achievement of objectives.

Ref	Question	Scoring
11.1	Are there processes in place to select, develop, operate and maintain the organisation's technology? Are they appropriate for the nature and extent of the technology used?	
11.2	Has the organisation identified each system that performs a role in the processing of transactions underlying significant accounts or disclosures and established IT general controls over those systems?	
11.3	Does the organisation have controls over IT application acquisition, implementation and maintenance? If so, consider:	
11.3.1	Whether formal policies and procedures are in place that define an approach to systems acquisition and change management (e.g., a formal systems development methodology)	
11.3.2	Whether user department and IT department management approval is required before systems acquisition and change projects are undertaken	
11.3.3	Whether the IT department maintains project documentation, including systems requirements definitions, risk analyses and cost- benefit analyses	
11.3.4	Whether the systems acquisition and change management approach addresses security risks	
11.3.5	Whether the systems acquisition and change management approach addresses data conversion	
11.3.6	Whether environments for development (or modification) and testing of IT solutions are separated (either logical or physical) from production systems	
11.3.7	Whether users are actively involved in the test process	
11.3.8	Whether development personnel are prohibited from migrating applications and data from the test environment to production	
11.3.9	Whether post-implementation review procedures are performed for system modifications made during an emergency	
11.4	Do policies and procedures exist and are they followed with regard to obtaining and implementing patches to operating system, database and application software?	
11.5	Does the organisation have controls over access to IT systems? If so consider:	
11.5.1	Whether formal policies and procedures are in place that define an approach to system security (including confidentiality of data and information)	
11.5.2	Whether a mechanism is in place for communicating security policies to employees (e.g., requiring users to sign an acknowledgement that they have read and understood the organisation's security policies)	
11.5.3	Whether a security organisation exists that is independent of both the user departments and other IT department functions	
11.5.4	Whether IT department personnel do not have operational or accounting responsibilities	
11.5.5	Whether appropriate user department and IT department management control access to the following: • Entity networks • Remote connection to networks and/or applications • Internet/intranet sites • Applications and application modules	

Scoring Guidelines: 10 Strongly Agree; 7 Mostly Agree; 5 Neither Agree nor Disagree; 3 Mostly Disagree; 0 Strongly Disagree

CONTROL ACTIVITIES: Technology Controls (2 of 2)

The organisation selects and develops general control activities over technology to support the achievement of objectives.

Ref	Question	Scoring
11.5.6	Whether the following user account security parameters are in place: • Users are assigned unique user IDs • Adequate passwords are required (e.g., minimum and maximum password length, at least one alpha and one numeric character) • Periodic password changes are required • User accounts are disabled after a limited number of unsuccessful logon attempts • Users are limited to one session per account (e.g., concurrent sessions or logons are not allowed) • Measures are in place to prevent the repeated use of a password • Administrator rights are assigned to a limited number of individuals who require those rights to perform their job duties	
11.5.7	Whether system security settings are configured to protect the entity's information	
11.5.8	Whether documented standards exist and are followed for the setup of new servers	
11.5.9	Whether access to security settings is limited to appropriate IT personnel	
11.5.10	Whether communications with public networks are controlled by a firewall. The firewall is implemented to: • Hide the structure of the client's network • Provide an audit trail of communications with public parties • Generate alarms when suspicious activity is suspected • Defend itself and/or the organisation's network against attack	
11.5.11	Whether procedures for protection against malicious programs are in place through the use of anti-virus software and other measures (which may include policies limiting the installation of unapproved programs, procedures for reporting suspected occurrences of viruses, etc.)	
11.5.12	Whether physical access to technology infrastructure is restricted	
11.5.13	Whether access to internal networks and/or applications by suppliers, customers, and/or other business partners is approved by appropriate management and limited to those networks and/or applications required to conduct business	
11.5.14	Whether representatives of suppliers, customers and/or other business partners are required to adhere to the client's policies, procedures, and security standards when accessing the client's systems	
11.6	Do the IT general controls identified appropriately consider the technology infrastructure in use (e.g., backups of applications, databases and operating systems are performed at appropriate intervals and periodically tested for recoverability)?	
11.7	Are responsibilities clear for initiating processing jobs (including subsequent checking for full completion) relating to internal transactions (e.g., invoicing) and the loading of third-party information (e.g., pricing data)?	
11.8	Are the IT general controls identified appropriate to address the risks posed by complete system replacement or extensive revision, where relevant?	
11.9	Has the organisation identified appropriate technology controls to address the risks of using applications hosted by third-parties?	

Scoring Guidelines: 10 Strongly Agree; 7 Mostly Agree; 5 Neither Agree nor Disagree; 3 Mostly Disagree; 0 Strongly Disagree

CONTROL ACTIVITIES: Policies and Procedures

The organisation deploys control activities through policies that establish what is expected and in procedures that put policies into action.

Ref	Question	Scoring
12.1	Has the organisation developed and documented policies and procedures for all significant financial statement accounts and disclosures? For example:	
12.1.1	Rationale for the policy, including risks to the financial statements	
12.1.2	Locations, units and processes to which the policies relate	
12.1.3	Clearly established responsibilities and accountability related to the execution of a particular policy/procedure, including the precision by which the policy/procedure is intended to operate	
12.1.4	Corrective actions to be taken as part of performing the activity	
12.1.5	Procedures for follow-up on exceptions identified	
12.1.6	Skills and level of authority required of person(s) performing the control	
12.1.7	Expectations regarding timeliness of performance of a control and any necessary follow-up	
12.1.8	Expectations for the documentation/evidence required to be maintained to support performance of the control	
12.2	Do the entity's policies and procedures include the following:	
12.2.1	Accounting and closing practices that are followed consistently at interim dates (e.g., quarterly, monthly) throughout the year?	
12.2.2	Is there appropriate involvement by management in reviewing significant accounting estimates and support for significant unusual transactions and non-standard journal entries?	
12.2.3	Is there timely and appropriate documentation for transactions?	
12.2.4	Does management review key performance indicators (e.g., budget, profit, financial goals, operating goals) regularly (e.g., monthly, quarterly) and identify significant variances?	
12.2.5	Does management investigate significant variances and is appropriate corrective action taken?	
12.2.6	Are variances in planned performance communicated and discussed with the board of directors and/or the audit committee at least quarterly?	
12.2.7	Are financial statements submitted to operating management? Are they accompanied by analytical comments?	
12.2.8	Has management established procedures to prevent unauthorised access to, or destruction of, documents, records (including computer programs and data files), and assets?	
12.2.9	Is data processing access to non-data processing assets restricted (e.g., blank checks)?	
12.3	Does the organisation review its policies and procedures periodically to determine whether they continue to be appropriate for the organisation's activities and refresh them when needed?	
12.4	Does the organisation have formal policies and procedures in place that: • Define an approach to systems acquisition and change management? • Obtaining and implementing patches to the operating system, database and application software? (same area covered in 11.4) • Define an approach to system security (including confidentiality of data and information)?	

Scoring Guidelines: 10 Strongly Agree; 7 Mostly Agree; 5 Neither Agree nor Disagree; 3 Mostly Disagree; 0 Strongly Disagree

INFORMATION AND COMMUNICATION:
Provision of Information

The organisation obtains or generates and uses relevant, quality information to support the functioning of internal controls.

Ref	Question	Scoring
13.1	Has the organisation established information requirements to support the effective operation of internal control?	
13.2	Are such requirements at the relevant level and needed specificity to support the identification of relevant and reliable sources of information and data?	
13.3	Does the organisation consider both internal and external sources of data when identifying relevant data to use in the operation of internal control?	
13.4	Does management re-evaluate its information needs periodically?	
13.5	Do the organisation's information systems generate information that is of sufficient quality to support the effective operation of controls? For example, has management developed and implemented controls related to:	
13.5.1	Completeness and accuracy of data	
13.5.2	Capture of data at the necessary frequency	
13.5.3	Providing information when needed	
13.5.4	Protection of sensitive data	
13.5.5	Retention of data to comply with relevant business, audit and regulatory needs	
13.6	Does the organisation periodically review the quality of information to assess its reliability and timeliness?	
13.7	With respect to information obtained from external sources, does the organisation have controls to ensure:	
13.7.1	The external sources are appropriate	
13.7.2	Information is supported by evidence from the source	
13.7.3	Information is of sufficient quality to support the effective operation of the control	

Scoring Guidelines: 10 Strongly Agree; 7 Mostly Agree; 5 Neither Agree nor Disagree; 3 Mostly Disagree; 0 Strongly Disagree

INFORMATION AND COMMUNICATION:
Internal Communication

The organisation internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.

Ref	Question	Scoring
14.1	Is there training/orientation for new employees, or employees when starting a new position, to discuss the nature and scope of their duties and responsibilities? Does such training/ orientation include a discussion of specific internal controls they are responsible for?	
14.2	Has the organisation implemented policies and procedures that facilitate effective internal communication, including individual internal control authorities and responsibilities and standards of conduct across the organisation?	
14.3	Are there written job descriptions and reference manuals that describe the duties of personnel, including their internal control responsibilities? (also covered in 4.4)	
14.4	Does senior management communicate the organisation's financial reporting objectives clearly through the organisation so that other management and personnel, including non-employees such as contractors, understand their individual roles in the organisation, regardless of physical location?	
14.5	Does the organisation's messaging reinforce to all employees their roles in ensuring that internal control responsibilities are taken seriously?	
14.6	Is there a process to quickly disseminate critical information throughout the entity when necessary?	
14.7	Do communications between the board of directors and management facilitate their oversight of the organisation's internal control and include, for example: • Matters important to the assessment of risks to the achievement of the organisation's financial reporting objectives • Results of the organisation's monitoring programs	
14.8	Do members of the board of directors have direct access to employees without interference from management?	
14.9	Does internal audit have a direct line of communication to the audit committee?	
14.10	Is there a process for employees to communicate improprieties? Is the process well-communicated throughout the entity? Does the process allow for anonymity for individuals who report possible improprieties? Is there a process for reporting improprieties, and actions taken to address them, to senior management, the board of directors or the audit committee?	
14.11	Are policies and procedures established for and communicated to personnel at decentralized locations? Has management taken into account cultural, ethnic and generational differences in determining appropriate methods of communication?	
14.12	Is there periodic evaluation of the effectiveness of communications to ensure the methods are working?	

Scoring Guidelines: 10 Strongly Agree; 7 Mostly Agree; 5 Neither Agree nor Disagree; 3 Mostly Disagree; 0 Strongly Disagree

INFORMATION AND COMMUNICATION:
External Communication

The organisation communicates with external parties regarding matters affecting the functioning of internal control.

Ref	Question	Scoring
15.1	Does the organisation have processes in place to communicate relevant and timely information to external parties including shareholders, partners, owners, regulators, customers, financial analysts and other external parties?	
15.2	Does the organisation have a process in place to approve formal external communications prior to their release?	
15.3	Is there a process for tracking communications from customers, vendors, regulators, and other external parties and sharing it internally?	
15.4	Is information from external parties about the organisation's activities that relates to matters of internal control evaluated by management and, where appropriate, communicated to the board of directors or the audit committee?	
15.5	Does the organisation have separate communication channels outside of the normal operations available to customers, suppliers and outsourced service providers to allow them to communicate directly with management and other personnel (such as a whistleblower hotline)?	

Scoring Guidelines: 10 Strongly Agree; 7 Mostly Agree; 5 Neither Agree nor Disagree; 3 Mostly Disagree; 0 Strongly Disagree

MONITORING ACTIVITIES: Ongoing Evaluation

The organisation selects, develops and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.

Ref	Question	Scoring
16.1	Does management have suitable monitoring processes in place to assess whether controls across the entire control framework are present and functioning as intended?	
16.2	Does this monitoring include evaluations built into business/financial reporting processes and performed on a real-time basis (ongoing evaluations) as well as separate evaluations performed periodically?	
16.3	Does the organisation's monitoring programs consider the following:	
16.3.1	The scope and nature of the organisation's operations	
16.3.2	The levels of risk throughout the entity (e.g., the level of risk by location, by business unit, by business process)	
16.3.3	The frequency and significance of changes in the organisation's operations	
16.4	Does the organisation's monitoring activities provide for the establishment of the understanding of the design and current state of the internal control system (e.g. performance of walkthroughs)? Is that understanding updated periodically?	
16.5	Are the results of monitoring activities considered over time to determine the basis for future monitoring activities?	
16.6	Is the level of staffing, training and specialized skills of the people performing the monitoring adequate given the environment (e.g., use of experienced, trained information systems auditors in complex and highly automated environments)?	
16.7	Is an internal audit function used as part of the organisation's monitoring program? If so:	
16.7.1	Is it independent (in terms of authority and reporting relationships) of the activities the function audits?	
16.7.2	Do internal auditors have direct access to the board of directors or audit committee?	
16.7.3	Is the scope of internal audit activities appropriate given the nature, size and structure of the organisation?	
16.8	Are there other quasi-audit functions (e.g., credit review in a financial institution or risk management in an insurance company) that report to management and affect the overall control environment?	
16.9	Do the monitoring activities include observations, inquiries and inspection of evidence?	
16.10	Are periodic assessments of the security of the IT environment performed?	
16.11	Are procedures in place to monitor when controls are overridden and to determine whether the override was appropriate?	
16.12	Do the organisation's monitoring activities consider services performed by outsourced service providers?	

Scoring Guidelines: 10 Strongly Agree; 7 Mostly Agree; 5 Neither Agree nor Disagree; 3 Mostly Disagree; 0 Strongly Disagree

MONITORING ACTIVITIES: Deficiency Management

The organisation evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors as appropriate.

Ref	Question	Scoring
17.1	Is there a process in place to accumulate and evaluate matters identified by the organisation's monitoring activities?	
17.2	Does this process include consideration of any themes underlying the identified deficiencies as well as potential root causes?	
17.2	Does the organisation receive findings and recommendations from external parties such as regulators, customers, vendors and external auditors? Is there a process in place for evaluating these matters?	
17.3	Are deficiencies communicated to those parties responsible for taking corrective action, senior management and the board of directors (or audit committee)?	
17.4	Are the results of internal audit activities reported to the following, as appropriate (and in accordance with the relevant reporting requirements): a) Senior management b) Board of directors or audit committee c) Independent auditors	
17.5	Are policies and procedures in place to ensure deficiencies are communicated externally, as required?	
17.6	Does management take adequate and timely actions to correct deficiencies reported by the internal audit function and by other monitoring activities?	
17.7	Does management respond timely and appropriately to the findings and recommendations of the independent auditors regarding internal control and policies and procedures of the organisation?	
17.8	Is there a process in place to track unremediated control deficiencies and a protocol to escalate them to higher levels of management if necessary?	

Scoring Guidelines: 10 Strongly Agree; 7 Mostly Agree; 5 Neither Agree nor Disagree; 3 Mostly Disagree; 0 Strongly Disagree

About ICE Integrated Control Environment

ICE is a GRC platform that helps cut the cost and complexity of managing your control and compliance environment.

It enables any organisation to manage its control and compliance environment with ease, freeing personnel from onerous, manual and inefficient activities - significantly reducing cost and enhancing quality.

C-level director and their risk, compliance and audit managers a strategic platform can manage and monitor the entire control and compliance environment, reducing the complexity of regulatory compliance and minimising the risk of control failures and potential non-compliance incidents.

What We Can Do for You

ICE was developed by Whitehall Management, a team of Finance, Business and IT professionals, working with internal and external auditors. We help companies to improve their control environments and to achieve and maintain compliance for stringent regulations such as SOX.

Our 'Roadmap to Control Excellence' is a professional, COSO-based review of your current control environment. It identifies gaps, inconsistencies or broken processes in your current control framework and guides you through the steps to enhance your control environment, improving performance and identifying opportunities to save costs.

For more details or to request a demo of how ICE can improve your organisation's control environment, contact:

Ross Baptie, Design & Delivery Director

Email: Ross.Baptie@ice-control.co.uk

Tel: 020 3368 3868

ICE
Integrated Control Environment